PATENT APPLICATION
DOCKET NO. PRIT01-00001

REMARKS

Please cancel claims 20 and 21 without prejudice to the Applicants. Claims 40 and 41 have been added. Claims 1-3, 5-7, 9-14, 16-19, 22-30, 34, and 36-39 have been amended. Accordingly, claims 1-19 and 22-41 are pending in the application.

Rejections Under 35 U.S.C. § 102

In paragraphs 1-6 of the Office Action dated September 30, 2004, the Examiner rejected claims 1, 2, 4, 5, 9-13, 16-22, 26-32, 38, and 39 under 35 U.S.C. § 102(b) as being anticipated by Young et al. (US 4,805,222). Claims 20 and 21 have been canceled. The Applicants have amended the remaining claims to distinguish the invention from Young. The Examiner's consideration of the amended claims is respectfully requested.

Young discloses a device and method that enables a computer system to verify the identity of a human user who is typing a password on the computer's keyboard. This is very different from the claimed invention, which enables an authentication device in a network to authenticate an automated user device.

Young initially generates a template for an individual user by measuring keystroke dynamics that are unique to the way the user types the password. The dynamics include measured time periods between the keystrokes, so that if a user has a unique rhythm in which he/she types the password, the rhythm becomes part of the template. The template is stored and whenever the password is typed again, the new keystroke dynamics are compared to the stored template. If the new keystroke dynamics match the stored template, the identity of the individual user is verified.

The process disclosed by Young requires that each individual keystroke be transmitted to the verification device as the keystroke is performed. This enables the verification device to measure the keystroke dynamics and determine whether the dynamics match the stored template. This process is not suitable for sending password

information over a network, and is quite different from the process utilized by the claimed invention. All network-based applications save bandwidth and reduce the time required to send the password over the network by temporarily retaining the password characters in local memory at the terminal until the user has finished typing the complete password and hits "enter" or "send". Only at that point is the password transmitted to the network verification device. Obviously, any keystroke dynamics such as time periods between the keystrokes are lost because the user terminal transmits the password in a single burst.

The Applicants' claimed invention solves this shortcoming of Young. While Young is designed to verify the identity of the individual user to a user device, the Applicants' claimed invention works at the next stage, that is, authenticating the user device to a server.

Claim 1 recites an apparatus for protecting a computer system. Claim 1 has been amended to recite that the apparatus includes a password controller coupled to the computer system, which is adapted to receive a password attempt transmitted from a user device over a network. The password controller operates a computer program to compare the password attempt with a stored password, which comprises a password segment. The password segment includes an entry event comprising a predetermined entry signal; a predetermined time interval following the entry event; and a terminating signal, which follows the predetermined time interval and marks the end of the password segment. The password controller allows the user device to access the computer system when the computer program determines that a password segment of the password attempt matches the password segment of the stored password.

Thus, the claimed invention is compatible with network-based applications in which the user device transmits the password over a network after the user enters it. The user device inserts the predetermined time interval between the entry event and the terminating signal, and thus is entirely different from Young, which measures time intervals as a user enters the password into the user device. These features are not taught or suggested by

Young. Therefore, the withdrawal of the rejection under § 102 and the allowance of amended claim 1 are respectfully requested.

Claims 2, 3, 5-7, 9, and 10 (also rejected under § 102) depend from amended claim 1 and recite further limitations in combination with the novel and unobvious elements of claim 1. Therefore, the allowance of claims 2, 3, 5-7, 9, and 10 is respectfully requested.

Independent claims 11 and 12 have also been amended to expressly recite that the password attempt is sent over a network, and that it is the user *device* that is being authenticated. Young verifies the user to the user device, not the user device to a network. Therefore, the allowance of amended claims 11 and 12 is respectfully requested for the reasons discussed above for claim 1.

Claims 13 and 16-19 (also rejected under § 102) depend from amended claim 12 and recite further limitations in combination with the novel and unobvious elements of claim 12. Therefore, the allowance of claims 13 and 16-19 is respectfully requested.

Independent claim 22 has also been amended to expressly recite that the password attempt is sent over a network, and that it is the user *device* that is being authenticated. Young verifies the user to the user device, not the user device to a network. Therefore, the allowance of amended claim 22 is respectfully requested for the reasons discussed above for claim 1.

Claims 23-29 (also rejected under § 102) depend from amended claim 22 and recite further limitations in combination with the novel and unobvious elements of claim 22. Therefore, the allowance of claims 23-29 is respectfully requested.

Independent claim 30 has been amended to recite a method of authenticating a user device in which an authentication device receives a password sent from the user device *in a single data burst transmitted after the user enters the complete password.* Thus no keyboard dynamics are considered. The password comprises a sequence of predefined characters, and the user device separates each of the characters by a predefined time interval from an adjacent character in the sequence. The method also

includes determining by the authentication device, whether the received characters match the predefined characters; determining by the authentication device, whether the received time interval between the received characters matches the predefined time interval; and positively authenticating the user device only if the received characters match the predefined characters, and the received time interval between the received characters matches the predefined time interval.

Thus, the claimed invention is compatible with network-based applications that transmit the password in a single burst after the user has typed in the complete password. In addition, in the claimed invention, it is the user device, not the user, which separates each of the characters from adjacent characters by a predefined time interval. These features are not taught or suggested by Young. Therefore, the withdrawal of the rejection under § 102 and the allowance of amended claim 30 are respectfully requested.

Claims 31 and 32 (also rejected under § 102) depend from amended claim 30 and recite further limitations in combination with the novel and unobvious elements of claim 30. Therefore, the allowance of claims 31 and 32 is respectfully requested.

Independent claim 38 has been amended to recite a method in a user device of constructing and transmitting a password utilized by an authentication device to authenticate the user device. The method includes the steps of receiving from a user, a sequence of predefined characters forming a password; identifying a predefined time interval for separating each character from an adjacent character in the sequence; and transmitting the password to the authentication device with each character being separated from the adjacent character in the sequence by the predefined time interval.

Thus, the claimed invention is compatible with network-based applications that transmit the password in a single burst after the user has typed in the complete password. In addition, in the claimed invention, it is the user device, not the user, which separates each of the characters from adjacent characters by a predefined time interval. These

features are not taught or suggested by Young. Therefore, the withdrawal of the rejection under § 102 and the allowance of amended claim 38 are respectfully requested.

Claim 39 (also rejected under § 102) depends from amended claim 38 and recites further limitations in combination with the novel and unobvious elements of claim 38. Therefore, the allowance of claim 39 is respectfully requested.

Rejections Under 35 U.S.C. § 103

In paragraphs 7-10 of the Office Action, the Examiner rejected claims 3, 6-8, 14, 15, 23-25, and 33-37 under 35 U.S.C. § 103(a) as being unpatentable over Young in view of Kung (US 5,241,594). The Examiner stated that Young shows the claimed invention except for an online connection to determine whether the password attempt from the online connection matches the stored password. The Examiner contends this feature is shown by Kung, and it would be obvious to combine the two references to obtain the claimed invention.

The Applicants respectfully disagree. First, claims 3 and 6-8 depend from amended base claim 1; claims 14 and 15 depend from amended base claim 12; claims 23-25 depend from amended base claim 22; and claims 33-37 depend from amended base claim 30. As noted above, Young does teach or suggest the limitations of the amended base claims. Therefore, the combination of Young and Kung fails to establish a *prima facie* case of obviousness because all of the recited limitations are not taught or suggested by the cited references.

Second, as noted above, Young is incompatible with systems that authenticate a user device over a network. The process disclosed by Young requires that each individual keystroke be transmitted to the verification device as the keystroke is performed. This enables the verification device to measure the keystroke dynamics and determine whether the dynamics match the stored template. This has to be done locally, between the user and the user device. Thus the combination of Young (which is local) with the online

connection of Kung is not proper. The Applicants contend that a person of ordinary skill in the art would not consider using the process disclosed by Young for a network application because it is too inefficient. Therefore, the withdrawal of the rejection under § 103 and the allowance of claims 3, 6-8, 14, 15, 23-25, and 33-37 are respectfully requested.

New Claims

New claim 40 depends from amended claim 38 and recites further limitations in combination with the novel and unobvious elements of claim 38. Therefore, the allowance of claim 40 is respectfully requested.

New claim 41 also depends from amended claim 1 and recites that the entry event comprises a plurality of sequential entry signals forming a data block, and the time interval follows the data block. Basis for new claim 41 is found in the originally filed specification in FIGS. 2B and 2C, which both show that the time interval is inserted after a plurality of entry signals forming a data block. This is entirely different from Young, which measures keystroke dynamics and time intervals between *individual* keystrokes as they are made by the user. Young does not teach or suggest inserting a time interval following a plurality of sequential signals. Therefore, the allowance of claim 41 is respectfully requested.

CONCLUSION

For all the above reasons, the Applicants respectfully request the allowance of claims 1-19 and 22-41 and the passing of this application to issue.

Respectfully submitted,

Steven W. Smith
Registration No. 36,684

Clyde R. Calcote
Co-Inventor

PATENT APPLICATION
DOCKET NO. PRIT01-00001

Attorney for James B. Pritchard
First-Named Inventor

Steven W. Smith
7237 Birchwood Drive
Dallas, Texas 75240
972-583-1572

Dated: December 10, 2004